International Journal of Computer Networking,
Wireless and Mobile Communications(IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 7, Issue 2, Apr 2017, 1-10

TRANS STELLAR
•Journal Publications •Research Consultancy

CONDITIONAL PROBABILISTIC POISSON FACTOR BASED MITIGATION MECHANISM FOR BYZANTINE ATTACK IN MANETS

GEETHA ACHUTHAN & SREENATH. N

Department of CSE, Pondicherry Engineering College, Puducherry, India

ABSTRACT

In wireless open structured multi-hop networks like Mobile Ad hoc Networks (MANETs), co-operation among the mobile nodes is the most significant entity for effective and reliable delivery of data packets. Due to its dynamic nature and open structure, MANETs are more vulnerable to security attacks. It is very easy for the adversaries to compromise the insider nodes and turn them as malicious that act arbitrarily to interrupt the network, besides referred to as Byzantine attacks. These authenticated Byzantine nodes may affect the routing process by selectively dropping the packets, modifying the packets and miss-routing packets and thus affects the overall network reliability. Moreover, the existence of byzantine mobile nodes in the network induces havoc impact on the level of co-operation established in the network. In this paper we propose a distributed mitigation mechanism based on Conditional Probabilistic Poisson Factor (CPPF) that analyzes and quantifies the reputation of each mobile node existing in the routing path. It detects the malicious nodes in all the routing paths based on the derived Probabilistic Oriented Poisson Factor value and also computes the reputation of routing paths and mitigates/avoids the byzantine nodes in routing. Extensive simulation results demonstrate the effectiveness of the proposed approach in mitigating Byzantine attacks in MANETs while providing better packet delivery ratio, throughput, reduced packet drop rate and overhead compared with other security protocols Cooperation of Nodes Fairness in Dynamic Ad-hoc.NeTworks (CONFIDANT), Cohen Kappa Reliability Coefficient based Reputation Mechanism (CKRCRM), CPPFMM detects and isolates byzantine nodes at the rate of 31% than the considered mitigation mechanisms.

KEYWORDS: Conditional Probability, Poisson factor, Byzantine Nodes, Co-Operation & Reputation

Received: Jan 10, 2017; **Accepted:** Feb 07, 2017; **Published:** Feb 22, 2017; **Paper Id.:** IJCNWMCAPR20171

Original Article

INTRODUCTION

In mobile ad hoc network, each mobile node relies on their neighbours for data delivery. In this network, nodes are free to move in an arbitrary fashion and hence the topology of the network is highly dynamic in nature [1-3].In the dynamic topology, the mobile nodes present in a particular range can communicate directly, whereas the nodes present outside the communication range make use of intermediate nodes to transfer a data packet to its destiny and this type of transmission may be called as multi-hop routing [4-5].In this multi-hop routing, the probability of a node participating in a routing activity is highly dependent on the reputation factor of the node [6-8]. The reputation factor of a mobile node reflects the reliability and cooperation of the particular mobile node to participate in a routing activity. But, there are some classes of mobile nodes which do not actively participate in the routing activity and drops the packets without transmitting to the next intermediate or to the destiny node [4]. In general, such classes of nodes are known as malicious nodes, which by its activity drastically reduce the network performance [9-12].

Our approach incorporates a distributed mitigation mechanism aiming at throughput degradation avoidance and packet drop rate reduction. It manipulates the reputation of each and every mobile node using Conditional Probabilistic Poisson Factor (CPPF) that quantifies the degree of co-ordination attributed by each of them. Our specific contributions are:

- We propose an estimation model to quantify the degree of co-opeartion rendered by the participating mobile nodes by using Conditional probabilistic Poisson Factor.
- We developed a Reputation mechanism for mitigating by zantine compromised nodes in order to maintain reliable network connectivity to sustain reslience of the ad hoc network.
- We implemented the proposed mechanism and analyze the overead of our solution in order to calculate its capability to alleviate the byzantine nodes and study the efficiency of our methodology.

The remaining part of the paper is organized as follows. Section 2 presents a brief literature review on the existing mitigation mechanisms proposed for detecting byzantine attacks in ad hoc networks. Proposed CPPFMM mechanism with its associated algorithms are elaborated in Section 3 and 4 .Section 5 presents the experimental results and the comparative study carried out with CKRCRM and CONFIDANT protocols. Section 6 concludes the paper with future plan of research.

CONDITIONAL PROBABILISTIC ORIENTED POISSON FACTOR BASED MITIGATION MECHANISM FOR BYZANTINE ATTACK IN MANETS (CPPFMM)

In this section, Conditional Probabilistic Poisson Factor based Mitigation Mechanism (CPPFMM) for Byzantine attack is presented. In CPPFMM, the detection of byzantine attack is achieved through mixed distribution that incorporates a conditional probabilistic approach that quantifies events that are modelled with discrete and continuous random variable. In other words, the computation of Poisson variated density function is based on the use of mixed distribution that employs the combination of discrete or continuous behaviour of mobile nodes. The mixed distribution is used mainly because the survivability of mobile nodes may happen discretely or continuously based on the source of influence originated by byzantine attacks.

Let us assume a Source Node ‘S’ wants to communicate with the destination node ‘D’, the source node ‘S’ broadcast control packets to all possible paths from ‘S’ to ‘D’ initially for establishing route discovery and route establishment. In this context, the lifetime of each routing paths $G(t)$ between the source and the destination depends on the individual lifetime of mobile node ($g(t)$). Further, the conditional probability $F_{X/Y}$ is evaluated based on discrete and continuous random behavioural analysis of mobile nodes that inspires Poisson and exponential distribution

First, the discrete behavioural analysis of mobile nodes are analysed based on Poisson distribution. This behavioural of mobile nodes depend on the availability of energy possessed by the mobile node towards routing. The amount of energy possessed by each mobile node is

$$AV_{energy} = \frac{E_U}{R_A} \tag{1}$$

Where AV_{energy}, E_U and R_A represents the amount of available energy, utilized energy and residual energy of

the mobile nodes. This energy parameter AV_{energy} is exponential distributed and the probability mass function $G(t)$ that pertains to the lifetime of each routing path based on lifetime $g(t)$ of mobile node is

$$G(t)_{(i)} = e^{-AVenergy}\left(\frac{(AV_{energy})}{PFNF}^{PFNF}\right) \tag{2}$$

In this context, PFNF denotes the packet forwarding Normalization Factor that ranges from 1 to 100.

Next, the behavioural analysis of mobile nodes is performed based on continuous distribution that inspires exponential distribution. The exponential distribution based probability mass function $CP_{s(i)}$ for identifying the resilience rate of mobile nodes of the network is

$$CP_{s(i)} = \kappa(1-P_{FC})^{\kappa-1} \tag{3}$$

Furthermore, $F_{X/Y}$ is computed based on two probabilities mass functions called $G(t)_{(i)}$ and $CP_{s(i)}$ are identified, they are integrated into an integral value that quantifies the impact of discrete and continuous analysis of lifetime of mobile nodes in each routing path is calculated using

$$F_{X/Y} = (G(t)_{(i)}) * (CP_{s(i)}) \tag{4}$$

Based on the above expression, the marginal density function with which a mobile node in any routing path exists is computed

$$f_X(t) = n(1-F_{X/Y})^{n-1} * P_Y(n) \tag{5}$$

Where 'n' and '$P_Y(n)$' refers to the number of nodes in the routing path and history reliability factor of the mobile nodes of the routing path respectively. Here, history reliability factor of the mobile nodes of the routing path refers to the normalized packet delivery rate of mobile nodes observed for a number of sessions

By the theorem of total probability, the reputation of each and every node at any time't' in a route discovered routing path is calculated through

$$R_{(X)}(t) = 1 - \sum_{t=0}^{\infty} f_X(t) \tag{6}$$

Based on the value of ($R_X(t)$), byzantine malicious nodes are isolated from the routing path. This Factor quantifies the likelihood probability for a mobile node to get infected into a byzantine node.

Simulations and Experimental Analysis

In this section, the performance analysis of the proposed CPPFMM is implemented with AODV. It is evaluated through simulation experiments using ns2(v. 2.26).The mobile nodes ranging from 50 to 100 are randomly distributed in the network area of 1000x1000 sq.meter.The nodes travel in the network according to the random way point mobility model which generates more realistic node movement patterns. The traffic pattern of the simulated network model is

represented in terms of constant bit rate (CBR) of 40 packets per second, the simulation time is set to 250 seconds. The performance of the proposed CPPFMM is evaluated based on performance evaluation parameters viz., packet delivery ratio, throughput, packet drop rate, total overhead and control overhead[13-15].

RESULTS AND ANALYSIS

Performance Evaluation of CPPFMM by Varying the Number of Mobile Nodes (Experiment 1)

In our first experiment, the number of mobile nodes is varied from 20 to 100 in increments of 20 in which 10% of the mobile nodes are byzantine compromised. The Figures 1, 2, 3 and 4 depicts the plots of packet delivery ratio, throughput, packet drop rate, total overhead and control overhead of CPPFMM obtained by comparing it with the byzantine mitigation mechanisms like CKRCRM and CONFIDANT.

CPPFMM shows considerable improvement in packet delivery rate when compared to the other mechanisms. CPPFMM exhibits an increase in PDR from 10%-12% than CKRCRM and from 19% to 25% than CONFIDANT. Figure 2 depicts the plots of throughput and it decreases when the number of byzantine nodes increases since increase in packet drop rate reduces the throughput. The proposed approach considerably increases the throughput of the network when compared to CKRCRM and CONFIDANT. CPPFMM shows an increase of 19% to 22% in throughput than CKRCRM and 26% to 29% than CONFIDANT. Further Figure 3 depicts the plots of packet drop rate for a given number of mobile nodes obtained from all the three byzantine mitigation mechanisms. However, the proposed CPPFMM approach considerably decreases the packet drop rate due its inbuilt prediction mechanism for analyzing behavioural changes of mobile nodes. CPPFMM shows a decrease of 12% to 16% than CKRCRM and from 25% to 29% than CONFIDANT.

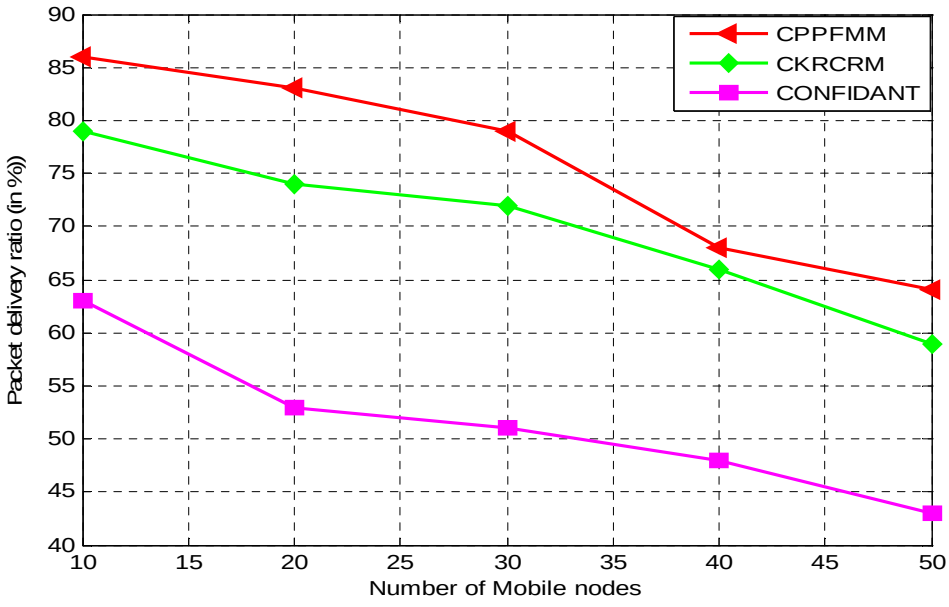

Figure 1: Performance of CPPFMM Based on Packet Delivery Ratio Obtained by Varying the Number of Mobile Nodes

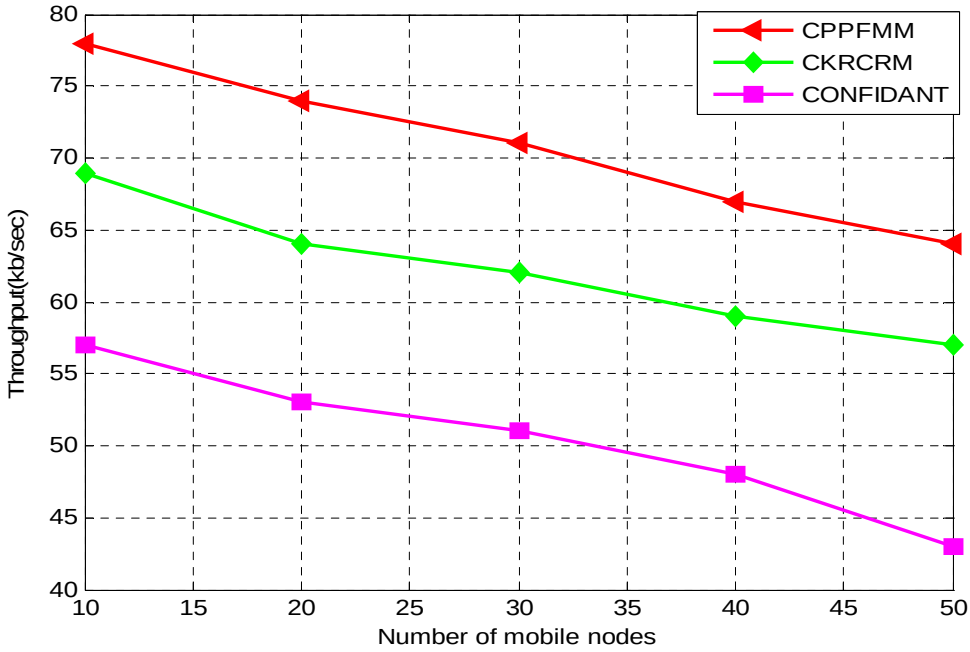

Figure 2: Performance of CPPFMM Based on Throughput Obtained by Varying the Number of Mobile Nodes

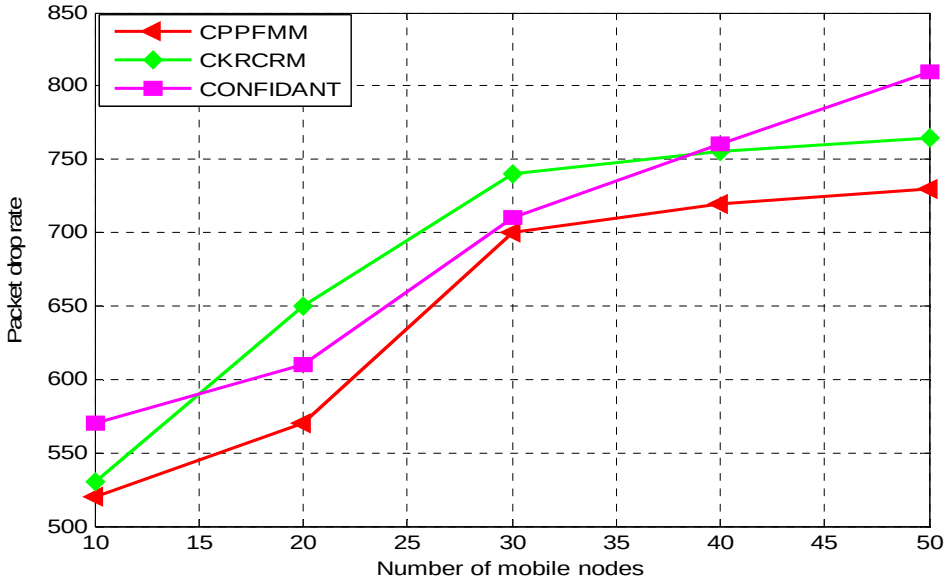

Figure 3: Performance of CPPFMM Based on Packet Drop Rate Obtained by Varying Number of Mobile Nodes

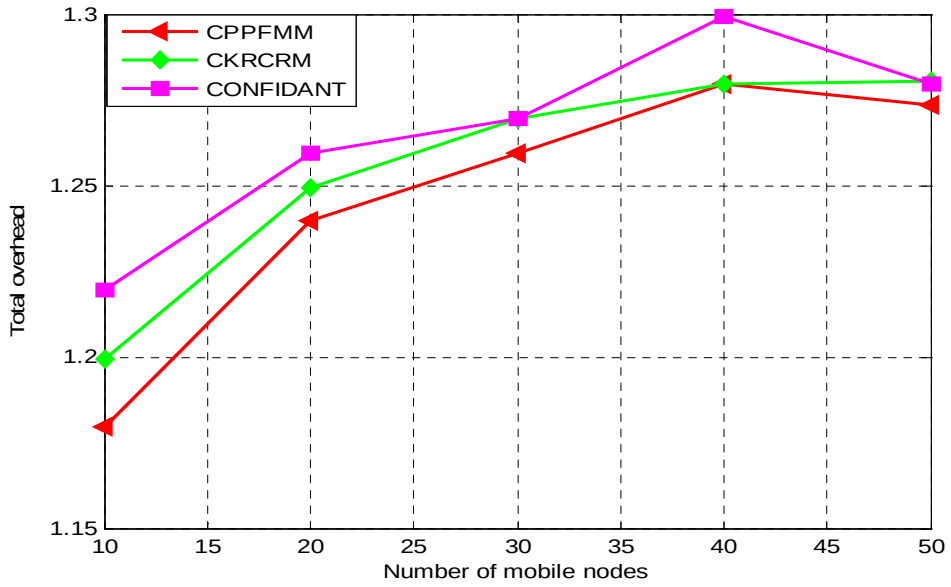

Figure 4: Performance of CPPFMM Based on Total Overhead Obtained by Varying Number of Mobile Nodes

Figure 4 depicts the plots of total overhead. The proposed CPPFMM approach shows a significant decrease in total overhead, since it isolates byzantine nodes and enables reliable routing path for data transmission. CPPFMM shows a decrease of9% to 12% than CKRCRM and from 18% to 22% than CONFIDANT. It decreases the total overhead by 26% when compared to the other two mechanisms.

Performance Evaluation of CPPFMM by Varying the Number of Byzantine Nodes (Experiment 2)

The second experimental analysis is carried by varying the number of byzantine nodes from 5 to 25 in the increments of 5 and the obtained results are depicted from Figures 5, 6, 7 and 8 respectively.

Figure 5 shows the decrease in packet delivery ratio (PDR) exhibited by all the above said three mitigation mechanisms when the number of byzantine nodes increases in the ad hoc environment. The proposed CPPFMM shows a considerable improvement in PDR compared to the other two mechanisms by 22.5%.It shows an increase in PDR from 13% to 17% than CKRCRM and from 24% to 28% than CONFIDANT. Figure 6 represents the throughput obtained by all the three considered mechanisms. The proposed CPPFMM approach considerably increases the throughput of the network by 18% compared to CKRCRM and CONFIDANT.

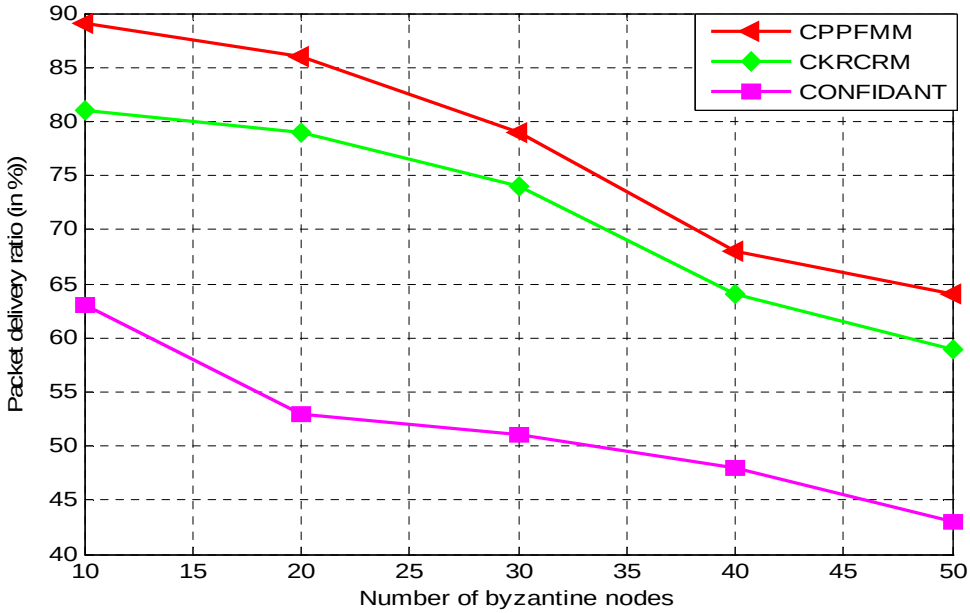

Figure 5: Performance of CPPFMM Based on Packet Delivery Ratio Obtained by Varying the Number of Byzantine Nodes

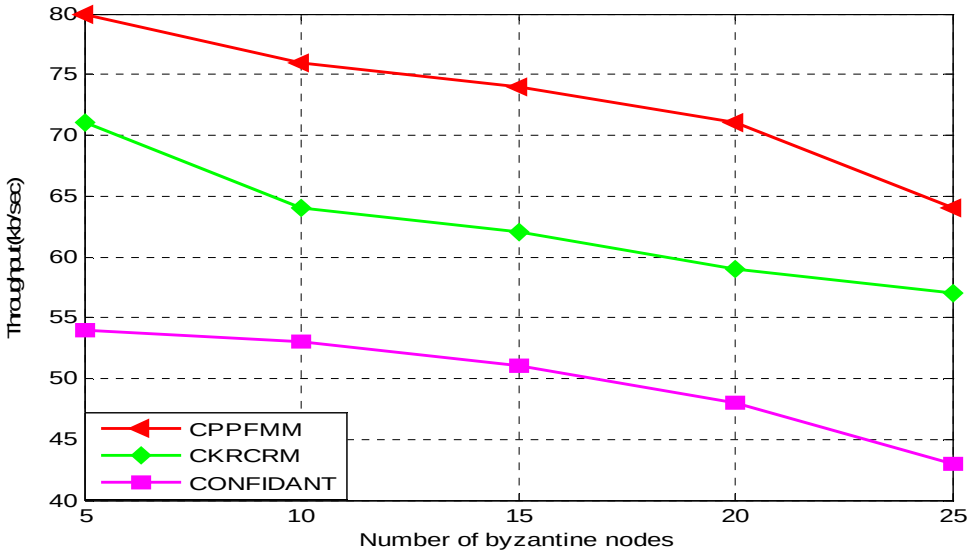

Figure 6: Performance of CPPFMM Based on Throughput Obtained by Varying Number of Byzantine Nodes

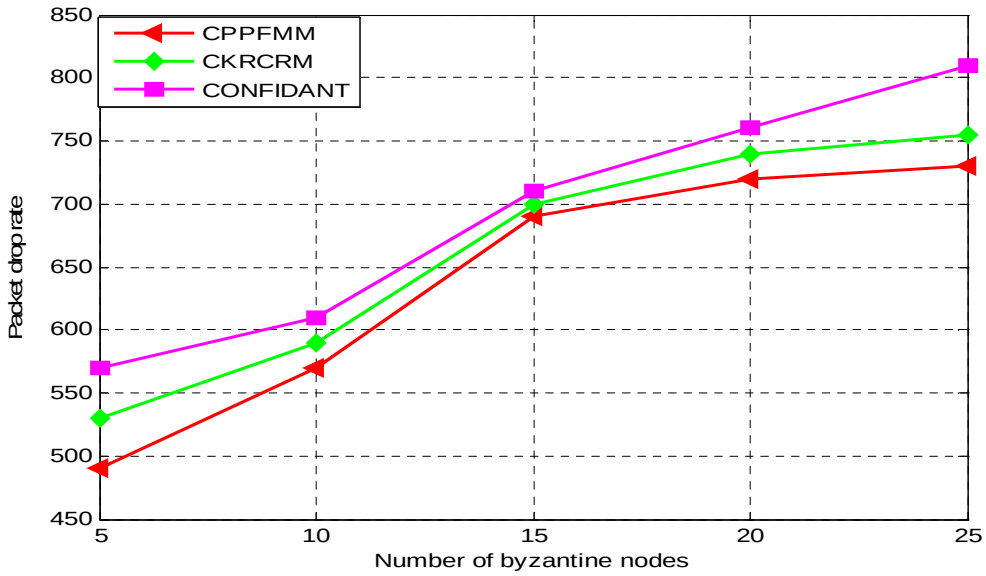

Figure 7: Performance of CPPFMM Based on Packet Drop Rate Obtained by Varying Byzantine Nodes

Figure 7 depicts packets drop rate, the packet drop rate generally increases when the number of byzantine nodes increases since they do not forward or cooperates with the other mobile nodes present in the routing path and drops the packets intentionally. The proposed CPPFMM approach considerably decreases the packet drop rate in an average by 26%, than the other two mechanisms. It decreases the packet drop rate from 9% to 12% than CKRCRM, and from 16% to 19% than CARFRMM and from 21% to 27% than CONFIDANT.

CONCLUSIONS

Securing MANETs is a really big challenge due to its open architecture. In this paper we have presented a new approach to mitigate the byzantine nodes by using a Conditional Probabilistic Poison Factor (CPPF).The experimental results confirms that this conditional probabilistic approach outperforms the CONFIDANT security protocol and CKRCRM in terms of throughput, control overhead, total overhead, packet delivery ratio and packet drop rate. CPPFMM in an average improves the packet delivery ratio by 15.6 % and throughput by25.4 % and at the same time, it reduces the total overhead, packet drop rate and control overhead by 19.5%, 39% and 31%, compared with the considered security mechanisms. Further CPPFMM detects and isolates the byzantine nodes rapidly at the rate of 31% which is remarkable.

REFERENCES

1. *Fei Xing, and Wenye Wang, On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviours and Failures. IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 3, pp. 284-299, (2010).*
2. *Md. Akhtar, A.K and Sahoo.G, Mathematical model for the detection of byzantine nodes in MANETs. International Journal of Computer science and Informatics, Vol. 1, No. 3, pp. 25 – 28,(2008).*
3. *Buchegger, S and Boudec, J-Y., Nodes bearing Grudges: Towards routing security, Fairness and Robustness in Mobile Ad-Hoc Network. Presented at tenth Eurominicro workshop on Parallel, Distributed and Network based Processing, Canary Islands, Spain, (2002).*

4. *Marti, S., Giuli, T.J., Lai, K., and Baker, M., Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking, Vol. 1, No. 1, pp.255–265, (2000).*
5. *Corradi, G., Janssen, J., and Manca, R., Numerical Treatment of Homogenous Semi-Markov rocesses in Transient Case – A Straightforward Approach, Methodology and Computing in Applied probability, vol.6, pp. 233-246, (2004).*
6. *Sundarajan, T and Shanmugam, A, Modeling the Behavior of ByzantineForwarding Nodes to Simulate Cooperation in MANET, International Journal, vol. 2, no. 2, pp. 147-160, (2010).*
7. *Fei Xing, Wenye Wang, Modelling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes. in prod., of IEEE International Conference on Communications, Vol. 4, No.3, pp.1879– 1884, (2006).*
8. *Alvaro A., C´ardenas, Svetlana Radosavac and JohnBaras, S., Evaluation of Detection Algorithms for MAC Layer Misbehaviour: Theory and Experiments. IEEE Transactions on Networking, Vol. 17, No. 2, pp.605-617, (2009).*
9. *Rohith Dwarakanath Vallam, Antony Franklin. A and Siva Rammurthy. C. 2008. Modelling Co-operative MAC Layer Misbehaviour in IEEE 802.11 Ad Hoc Networks with Heterogeneous Loads. In prod.,6th International Symposium on Modelling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, WIOPT Berlin, Germany, Vol. 1, No. 1, pp. 197-206.*
10. *Neeraj Jaggi, Vamshikrishna Reddy Giri and Vinod Namboodiri. Distributed Reaction Mechanisms to Prevent ByzantineMisbehavior in Wireless Ad Hoc Networks. in proc of the Global Communications Conference, GLOBECOM 2011, Houston, Texas, USA. IEEE, Vol. 1, No. 1, pp. 1-6, (2011).*
11. *Hernandez-Orallo, E., Serraty, M.D., Cano, J-C., Calafate, T.and Manzoni, P. Improving byzantine node detection in MANETs using a collaborative watchdog. IEEE Letters,. Vol. 16, No. 5, pp. 642-645, (2012).*
12. *TaragFahad and Robert Askwith., 'A Node Misbehaviour Detection Mechanism for Mobile Ad hoc Networks', PGNet. (2006).*
13. *Buchegger,S and J. Boudec, Performance Analysis of the Confidant Protocol, in Proc. Int'l Symp, Mobile Ad Hoc Networking and Computing(2002)*
14. *Geetha,A and Sreenath,N., "Cohen Kappa Reliability Coefficient Based Mitigation Mechanism For Byzantine Attack In MANETs". International Journal of Applied Engineering Research, vol 10, no 9, pp. 23989-24001, (2015).*
15. *Sathiyamoorthy, E., Narayana, N.C.S., and Ramachandran, V., "Agent Based Trust Management Model Based on Weight Value Model for Online Auctions", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No.3, October2009.*